



QUICK START GUIDE

## IM7200 and IM7200-L

Includes: IM7208, IM7216, IM7232, IM7248  
and all IM7200-L models



03212019

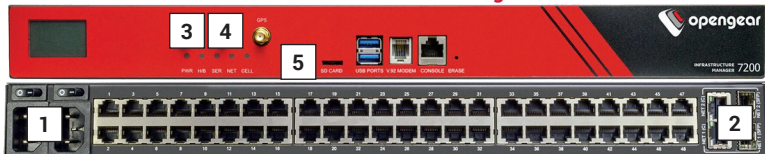
# 1. REGISTER

Register your product: <https://opengear.com/product-registration>

For licensing information and access to source code, visit:  
<https://opengear.com/software-licenses>

# 2. WHAT'S IN THE BOX?

## 48 Port Infrastructure Manager



1. POWER SWITCH & POWER SUPPLY
2. NET1 & NET2
3. CELL (MAIN)
4. CELL (AUX)
5. SIM CARD SLOT
6. 24 USB console ports (IM7216-2-24U-DAC)
7. 24 Port Gigabit Switch (IM7216-2-24E-DAC)

## 16 Port + 24 USB Port Unit



## 16 Port + 24 Port Gigabit Switch





Note: Antenna only included with -L models

For the complete list of what's inside the box, visit:

<https://opengear.com/products/im7200-infrastructure-manager#inside>



**After opening the box:**

**DO NOT POWER ON RIGHT AWAY**

### **3. CONNECT**

Connect the NET1 port to your network. The NET2 port is inactive by default. Refer to the User Manual for instructions to activate it.

### **4. POWER UP**

Plug the AC power cable into the unit and connect to a power source. Turn on the switch above the outlet. DAC models have two power switches.

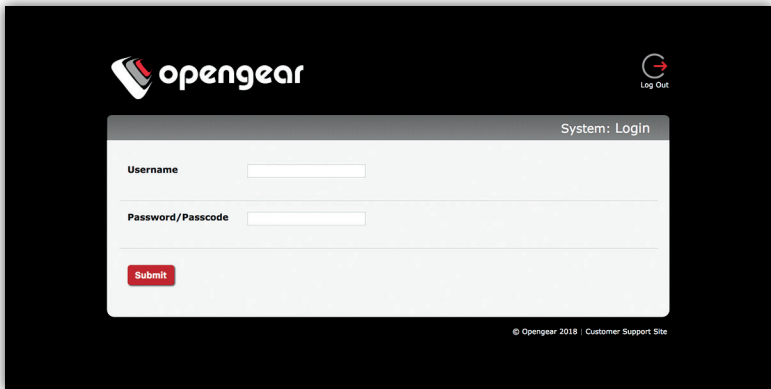
DDC models have dual DC power supplies with automatic failover. Connect these to DC power sources with the included external screw connector blocks.

**For -L models,** attach the included antennas or external mount to the CELL (MAIN) and CELL (AUX) connectors. If you have a data plan, insert a carrier-provided mini-SIM into the SIM CARD slot with contacts facing downward. You should hear a click when it is correctly inserted.

## 5. LOG IN

Browse to **192.168.0.1** (subnet mask 255.255.255.0) with a computer on the same LAN as the console server. The device will also get a DHCP address.

NOTE: The device has a self-signed SSL certificate. Untrusted connection errors appear. Click through the errors to the login page.



opengear

Log Out

System: Login

Username

Password/Passcode

Submit

© Opengear 2018 | Customer Support Site

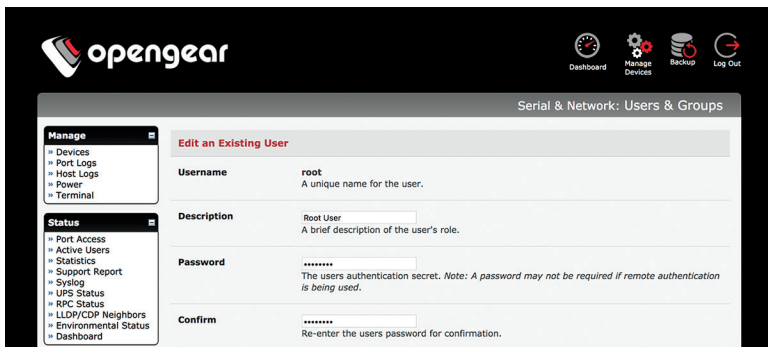
Log in with username **root** and password **default**. Click **Submit**.

You will now see a Welcome screen with a list of basic configuration steps.

## 6. CHANGE ROOT PASSWORD

Click **Serial & Network > Users & Groups**.

Click Edit next to the root user. On the **Edit an Existing User** page, enter and confirm your new password.



The screenshot shows the OpenGear web interface. At the top left is the OpenGear logo. On the top right are navigation icons for Dashboard, Manage Devices, Backup, and Log Out. The main header reads "Serial & Network: Users & Groups". On the left is a sidebar with "Manage" and "Status" sections. The "Manage" section includes: Devices, Port Logs, Host Logs, Power, and Terminal. The "Status" section includes: Port Access, Active Users, Statistics, Support Report, Syslog, UPS Status, RPC Status, LLD/CDP Neighbors, Environmental Status, and Dashboard. The main content area is titled "Edit an Existing User" and contains the following form fields:

<b>Username</b>	root A unique name for the user.
<b>Description</b>	Root User A brief description of the user's role.
<b>Password</b>	***** The users authentication secret. <i>Note: A password may not be required if remote authentication is being used.</i>
<b>Confirm</b>	***** Re-enter the users password for confirmation.

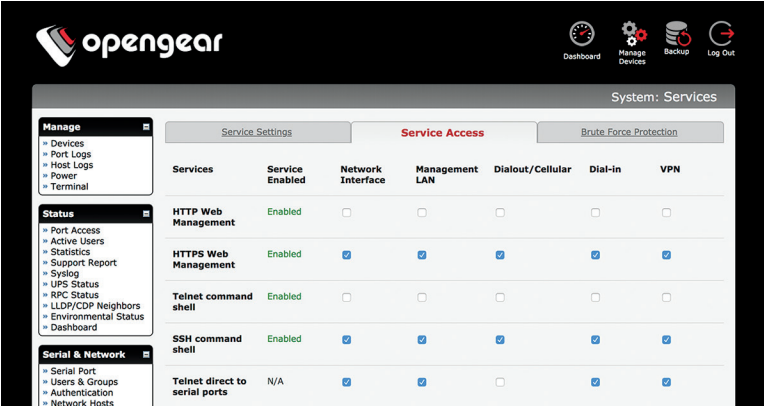
Scroll to the bottom of the page and click **Apply**.

## 7. CHANGE IP SETTINGS

DHCP is enabled by default. If you need to change to a static IP, click **System > IP**. Under the **Network Interface** tab, change the **Configuration Method** to Static IP.

## 8. CHANGE ACCESS & FIREWALL SETTINGS

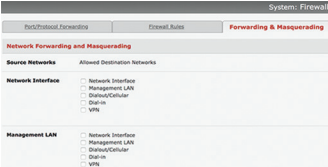
The console server's firewall controls which protocols and services can access which ports and devices. By default, the firewall only allows HTTPS and SSH access. To change settings, click **System > Services** and click the **Service Access** tab.



The screenshot shows the OpenGear console interface. The top navigation bar includes the OpenGear logo and icons for Dashboard, Manage Devices, Backup, and Log Out. The main content area is titled "System: Services" and has three tabs: "Service Settings", "Service Access" (selected), and "Brute Force Protection".

The "Service Access" tab displays a table with the following columns: Services, Service Enabled, Network Interface, Management LAN, Dialout/Cellular, Dial-in, and VPN.

Services	Service Enabled	Network Interface	Management LAN	Dialout/Cellular	Dial-in	VPN
HTTP Web Management	Enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HTTPS Web Management	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Telnet command shell	Enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SSH command shell	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Telnet direct to serial ports	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



The screenshot shows the "System: Firewall" page with the "Forwarding & Masquerading" tab selected. The page is titled "Network Forwarding and Masquerading" and contains settings for "Source Networks" and "Allowed Destination Networks".

**Source Networks**

- Network Interface
- Management LAN
- Dialout/Cellular
- Dial-in
- VPN

**Management LAN**

- Management LAN
- Management LAN
- Dialout/Cellular
- Dial-in
- VPN

To permit IP access between devices on the network or management LAN, click **System > Firewall**. Click on the **Forwarding & Masquerading** tab, make any changes, and click **Apply**.

## 9. CONFIGURE SERIAL & USB DEVICES

Click **Serial & Network > Serial Port**. Click **Edit** to modify a specific port.

Serial & Network: Serial Port							
Port #	Label	Connector	Mode	Logging Level	Parameters	Flow Control	
1	Port 1	RJ45	SDT ( <i>root</i> )	3	115200-8-N-1	None	<a href="#">Edit</a>
2	catalystswitch	RJ45	Console ( <i>SSH, Web Terminal</i> )	3	9600-8-N-1	None	<a href="#">Edit</a>
3	Port 3	RJ45	Console ( <i>SSH, Web Terminal</i> )	0	115200-8-N-1	None	<a href="#">Edit</a>

You can modify common settings including Baud Rate, Parity, Data Bits, Stop Bits, and Flow Control as well as port connection settings including SSH, Telnet, Web Terminal, and RFC2217.

The IM7200 also offers a software-selectable pin out (Port PinOut).

Click **Apply** to save any modified settings.

**NOTE:** Your console server has two USB 3.0 ports which can be connected to USB consoles on UPS supplies or Cisco devices. They may also be used with external USB flash drives to update firmware and configuration files. The IM7216-2-24U also has 24 rear-facing ports that support device console management via USB.



## 10. ADD USERS AND GROUPS

To add a new user, click **Serial & Network > Users & Groups**. Scroll to the bottom of the page and click **Add User**.

Enter a **Username** and enter and confirm a **Password**. Select the appropriate groups and scroll down to choose the **Accessible Ports** the user is allowed to access.

Serial & Network: Users & Groups

---

**Add a New user**

**Username**   
A unique name for the user.

---

**Description**   
A brief description of the user's role.

---

**Groups**

- admin (Provides users with unlimited configuration and management privileges)
- pptpd (Group to allow access to the PPTP VPN server - Users in this group will have their password stored in clear text.)
- dialin (Group to allow dialin access via modems - Users in this group will have their password stored

Click **Apply** to create the new user account.

**NOTE:** You should create a new administrative user rather than continuing as the root user. To do so, add a new user to the **admin** group with full access privileges. Log out and log back in as this new user for all administrative functions.

To create a new group, click **Serial & Network > Users & Groups**. At the end of the list of existing groups, click **Add Group**.

Enter a new group name in the **Groups** field. Select any appropriate **Roles, Hosts, Ports, and RPC outlets**.

Serial & Network: Users & Groups

---

**Add a New group**

**Groups**   
A group with predefined privileges the user will belong to.

**Description**   
A brief description of the group's role.

---

**Roles**

- Full administration & access
- Access to all serial ports and managed devices
- Web UI access to the 'Manage' pages
- CLI connections provide access to the Port Manager shell (This takes precedence over the UNIX Shell Role)
- CLI connections provide access to a UNIX shell

Click **Apply** to create the new group.

## 11. ACCESS DEVICE CONSOLES

Your console server is now ready to access device consoles on your network, depending on the protocols you chose in Step 9.

### SSH:

- To connect to the pmsHELL chooser menu, SSH to the console server and log in appending `:serial` to your username, e.g. `root:serial`.
- To connect to a given console, SSH to the console server and login adding the port number or port label to your username, e.g. `root:port02` or `root:MyRouter`.
- To connect directly to a given port, SSH to the console server at TCP port 3000 + the port number, e.g. 3002 for serial port 2.

### Telnet:

Telnet to the console server at TCP port 2000 + the port number, e.g. 2002 for serial port 2.

### Web Terminal:

For console access using your browser, click **Manage > Devices > Serial** and click the port's **Web Terminal** link.

## 12. USE CELLULAR MODEM (-L MODELS)

In the console, select **System > Dial**.

Click the **Internal Cellular Modem** tab.

Check the **Allow outgoing modem communication** radio button.

Enter your carrier's Access Point Name in the **APN** field.

If necessary, check the **Override returned DNS servers** box and enter your DNS's addresses.\*

Click **Apply Modem Dial Settings**.

\*If cellular is not the primary network route, you may need to override the provided DNS servers if you have issues with name resolution.

To check the status of the modem connection:

Select **Status > Statistics**.

Click the **Failover and Out-of-Band** tab.

Make sure the **Always on Out-of-Band -- Internal Cellular Modem's Connection Status** is Connected.

Check the modem's allocated IP Address to see if it is a public or private address.

You can find more information about cellular features in the Opengear Knowledge Base under the **FAQ > Cellular & Wireless** section.

[opengear.zendesk.com/hc/en-us/sections/203134783-Cellular-Wireless](https://opengear.zendesk.com/hc/en-us/sections/203134783-Cellular-Wireless)

This guide is designed to get you started. For complete instructions, download the User Manual from [https://ftp.opengear.com/download/manual/current/Opengear User Manual.pdf](https://ftp.opengear.com/download/manual/current/Opengear%20User%20Manual.pdf)

## LIGHTHOUSE CENTRALIZED MANAGEMENT

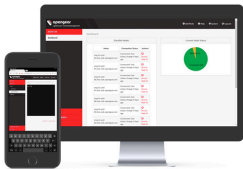
Lighthouse is a powerful tool that simplifies the way you manage your out-of-band network through a single pane of glass. Better control and visibility provides 24/7 resilient access to your connected IT infrastructure.

### Lighthouse features:

- Centralized scalable administration and automation of nodes
- Easy to maintain user groups and permissions
- Secure accessibility for all connections using Lighthouse VPN
- Responsive UI designed and built for NetOps
- Integrated RESTful API

“Deployment is made very easy as Lighthouse learns about attached devices during node enrollment and will dynamically update itself as new devices attach.”

– Network Computing Magazine Product Review – Dec 2017



### Ready to learn more?

Visit [lighthouse.opengear.com](https://lighthouse.opengear.com) to download a free evaluation of Lighthouse (up to 5 nodes) and to learn more about Opengear's Centralized Management solutions.